UNITED STATES DISTRICT COURT

SOUTHERN DISTRICT OF NEW YORK

WINKLEVOSS CAPITAL FUND, LLC, Plaintiffs, v. CHARLES SHREM, Defendant.	Case No. **AFFIDAVIT OF TOM ROBINSON IN SUPPORT EX PARTE APPLICATION FOR PREJUDGMENT ATTACHMENT** 18 CV 8250

I, Tom Robinson, declare as follows.

1. I am the Chief Data Officer, Lead Forensic Investigator, and co-founder of Elliptic, a cryptocurrency forensic intelligence firm. We were retained to provide investigatory services relating to Cryptocurrency transactions on the Bitcoin network by Charles Shrem. This declaration summarizes some of our findings. Except as to matters stated on information and belief, I have personal knowledge of the information referenced herein and could competently testify as to its truth if called to do so. As to matters stated on information and belief, I am informed and believe them to be true.

2. We work with both law enforcement and financial institutions to identify illicit activity on the Bitcoin blockchain. We have developed forensic techniques that eliminate some of the anonymity of the blockchain and we can sometimes trace bitcoin transactions to real-world individuals. We have delivered actionable intelligence to clients in both the United States and Europe and have amassed evidence in cases of arms trafficking, theft, money laundering and the illegal drug trade.

3. I am routinely consulted by major media outlets as an expert in Bitcoin and the blockchain, including the New York Times, the Guardian, CNN, ABC News, Bloomberg News, BBC News and other outlets. I hold a D.Phil in atomic and laser physics from the University of

Oxford. Attached hereto as Exhibit A is a true and correct copy of my C.V., which gives a more extensive overview of my professional background and expertise in Bitcoin and the blockchain.

4. In July 2017, Elliptic was engaged by Winklevoss Capital Management, LLC ("WCM") which provides services to Winklevoss Capital Fund ("WCF"), the family investment firm of Cameron and Tyler Winklevoss. WCF suspected that Charles Shrem, the former owner of BitInstant, had embezzled approximately 5,000 bitcoin from WCF when he agreed to purchase bitcoin on its behalf in late 2012 and early 2013. Elliptic was engaged to examine (a) whether we could identify Shrem's current bitcoin holdings, (b) whether we could identify any prior bitcoin transactions on the blockchain involving Shrem, and (c) whether we could identify bitcoin transactions by Shrem between September and December 2012 that might account for the missing bitcoin owed to WCF.

5. We reached two important conclusions. First, we identified a bitcoin transaction from an address controlled by Shrem that received 5,000 bitcoin in December 2012, in close proximity to the timeframe in which WCF alleges that Shrem embezzled approximately a similar amount. Tracing the subsequent movements of this bitcoin, we determined that approximately 4,000 of these 5,000 bitcoin moved into two bitcoin exchanges — Coinbase and Xapo — which would have additional information on the owner of the accounts that received the funds.

6. Second, we found evidence that Shrem has transacted with many of the major bitcoin exchanges. Shrem has publicly acknowledged personally purchasing thousands of bitcoin in the early days of the cryptocurrency.

Overview of bitcoin

7. Bitcoin is a digital currency created in 2009. Unlike traditional currency, there is no government that backs and issues the currency. Rather, the creation and administration of Bitcoin is decentralized like other peer-to-peer networks which rely on crowdsourcing to operate, such as BitTorrent. A diffuse network of users provides the computing power to run the Bitcoin network. In essence, they compete to record transactions in the blockchain and when they prevail

in that competition they are rewarded with the issuance of new bitcoin. This practice is called "mining." The competition ensures that only one party records a transaction on the blockchain so there is no chance of differing entries. An overview of the Bitcoin blockchain network from bitcoin.org is attached hereto as Exhibit B.

8. The network is at once radically public and relatively anonymous. Every bitcoin transaction that has ever taken place and that will take place is recorded on the public blockchain, a distributed ledger maintained by the computers on the Bitcoin network that provide processing power. The blockchain both records and is confirmation that a specific bitcoin address holds bitcoin, thus preventing double-spending or double-dipping. Specifically, for each transaction, the blockchain maintains a record of (1) the time of the transaction, (2) the amount of the transaction, and (3) the addresses involved in the transaction. Because the blockchain ledger is distributed, it cannot be altered or forged and the network as a system remains secure. In other words, every user's holdings are reflected by the blockchain, because the blockchain records all movements of bitcoin to and from each address.

9. Yet while the blockchain itself is radically public and transparent, bitcoin users' identities are not visible on the blockchain because users simply store and transfer bitcoin from a 25- to 34-character alphanumeric address. There are no names on the blockchain or other identifying information. Addresses can only be associated with an individual owner by cross-referencing the address with information extrinsic to the blockchain.

10. Each address, in turn, has a private key that allows an owner of an address to log into that address and transfer bitcoin to another address. Bitcoin transactions can also involve multiple addresses — if one user controls two addresses, that user may send bitcoin from two addresses to a third address. Likewise, users may transfer bitcoin from one address to multiple addresses in one transaction. There is no numeric limit on how many addresses may be involved in a single transaction.

Bitcoin exchanges

11. The Bitcoin ecosystem has evolved since its creation to include a number of vendors who act as custodians and/or virtual banks.

12. Because of the technical complexity of creating a bitcoin address, storing bitcoin and transacting in bitcoin, a number of Bitcoin companies, such as Gemini, Coinbase, and Xapo, offer user-friendly ways of buying, storing and selling bitcoin.

13. Rather than require a user to set up an actual bitcoin address on the blockchain, these services allow users to buy, store and sell bitcoin through their websites. These vendors handle the technical aspects of bitcoin — creating blockchain addresses, accessing those addresses with private keys, and transferring bitcoin — thereby allowing users to buy, sell and transfer bitcoin simply through the use of a bank account or credit card, and a login and password.

14. These companies also allow a user to store bitcoin in virtual wallets. The companies act as custodians over the bitcoin, enabling a user to hold bitcoin without requiring the user to set up a blockchain address and maintain a private key.

15. When a user (a) sends bitcoin to an exchange, (b) purchases bitcoin on an exchange, or (c) stores bitcoin on an exchange, the exchange typically holds those bitcoin on multiple addresses, or co-mingles one user's bitcoin on a single address with other users' bitcoin. So once bitcoin is transferred to an address controlled by one of the exchanges, it is difficult to associate that bitcoin with the individual beneficial owner of the coin. The exchange's internal ledger accounts for how many bitcoin are held by each user in the exchange.

16. Many of the exchanges — especially those operating in the United States and Europe — are required by financial transparency and anti-money laundering laws to obtain identifying information about their users. Therefore, the bitcoin exchanges know the identity of their bitcoin users; information that would not be apparent simply from looking at the blockchain.

Overview of Elliptic's Work

17. Despite the relative anonymity of the blockchain, our firm has pioneered several means of identifying a bitcoin user.

18. The most obvious way to figure out who owns a bitcoin address is if the owner acknowledges that they own a particular address. This can be done by open-source research on the web and the "dark web,"[1] as well as offline research connecting individuals to blockchain addresses.

19. At Elliptic, we constantly identify new addresses. Sometimes this is as simple as discovering that a store accepts bitcoin and associating a bitcoin address where the store accepts bitcoin with the store. We also transact directly with bitcoin services in order to gain insight on the addresses that they use.

20. Once one address has been identified, we can identify additional addresses through "clustering." Often times, one user owns multiple bitcoin addresses. When a transaction involves bitcoin being sent from two or more addresses to a third address, the two or more sending addresses are said to be a "cluster" and are under the control of a common owner. If we can identify one address in a cluster as being associated with an individual, we can thereafter identify the rest of the addresses in a cluster with that individual.

21. Elliptic has pioneered bitcoin forensics by utilizing these two tools — identifying bitcoin addresses and clustering. By using powerful computing software, we analyze all of the bitcoin transactions ever recorded on the blockchain. We update our analysis on a daily basis.

[1] The "dark web" is the part of the internet that cannot be accessed through traditional internet browsers such as google chrome or Microsoft internet explorer. It is an encrypted space on the internet. To access the dark web, an internet user must use a cloaking protocol, which provides access to encrypted and anonymized internet sites. Many black marketplaces and e-commerce sites selling illegal goods, such as drugs, weapons, and illegal pornography, are housed on the dark web. Because bitcoin can be used to transact without identifying the user, it is a useful currency on the dark web.

Winklevoss Project

22. In July 2017, we were retained by WCM to determine whether we could identify any bitcoin held by Charles Shrem. Shrem was an early bitcoin adopter who founded BitInstant in 2012, one of the first companies to facilitate bitcoin transactions for consumers. Shrem was also a founding member of the Bitcoin Foundation, an early non-profit group dedicated to promoting bitcoin. In 2014, Shrem pleaded guilty to felony money laundering charges for knowingly facilitating bitcoin transactions for drug dealers and other criminals on the dark web. *USA v. Faiella, et al.*, No. 14-CR-243, Dkt. No. 61, (S.D.N.Y. December 23, 2014) (Rakoff, J.).

23. The Winklevoss twins told us that between late 2012 and early 2013 they gave Shrem $750,000 to purchase bitcoin on behalf of their investment firm, WCF. The Winklevoss twins said they believed they received approximately 5,000 bitcoin less than they were owed, based on the fact that Shrem could not account for approximately $61,000 that they sent him between September and October 2012.

24. WCM asked us to determine whether we could (1) identify any bitcoin holdings of Shrem, (2) identify any prior bitcoin transactions with Shrem, and (3) determine whether Shrem acquired any bitcoin around late 2012 that might account for his 5,000 bitcoin shortfall.

25. The Winklevoss twins shared with us WCF's bitcoin transaction history with Shrem.

26. By utilizing our clustering software, this initial data set provided us with 167 addresses in 28 clusters that were the source of the bitcoins sent by Shrem.

27. Alongside this client-sourced information, we conducted independent research to look for additional bitcoin addresses associated with Shrem. We found thirteen additional addresses associated with Shrem based on this research.

28. We started by reviewing bitcointalk.org, a popular online forum for bitcoin users. Charles Shrem was an active user of this forum between 2012 and 2014, under the user ID "Yankee (bitinstant)."

29. In reviewing Shrem's posts on the forum, we were able to identify a further ten addresses associated with Shrem.

30. Of these ten addresses, we identified nine addresses based on a review of a message exchange between Shrem and another user who accused Shrem of being a scam artist and not delivering 60 bitcoin to him as promised. Shrem apparently made good on this debt and sent the disgruntled user 60 bitcoin over time. By analyzing the date and time that Shrem said that he sent bitcoin, and comparing that data with evidence on the blockchain, we identified certain addresses as likely belonging to Shrem. An extract of a copy of this exchange on bitcointalk.org is attached hereto as Exhibit C.

31. We identified one more address as belonging to Shrem from bitcointalk.org because he publicly acknowledged ownership the address.

32. Specifically, on April 2, 2014, the user "Yankee (bitinstant)" posted the following: "I own this address: 1Shremdh9tVop1gxMzJ7baHxp6XX2WWRW –Charlie Shrem." This was part of a discussion thread about "vanity addresses," i.e. bitcoin addresses containing a word or phrase within the address.[2] The fact that the address contains the word "Shrem" is further indication that the address, in fact, belongs to Shrem. A screenshot of that webpage, captured on December 8, 2017, is attached hereto as Exhibit D.

33. We identified another bitcoin address associated with Shrem after reviewing his twitter account. On July 28, 2017, Shrem acknowledged a transaction on twitter with Roger Ver. By cross referencing the details in Shrem's tweet about the amount and time of the transaction with transactions on the blockchain, we identified the transaction. This allowed us to identify the sending address as belonging to Shrem. A screenshot of Shrem's twitter feed acknowledging the transaction is attached hereto as Exhibit E, and a screenshot of the blockchain transaction is attached hereto as Exhibit F.

[2] *See* https://bitcointalk.org/index.php?topic=553449

34. We identified one additional address as belonging to Shrem after reviewing his personal webpage, charlieshrem.com. On his webpage, he includes a "donation" link where users can donate bitcoin to address 1CbfpkobnUWeNT6T4e3G9cwrdHbJ3SSiQU. We recorded this as an additional address belonging to Shrem.

35. It is likely that Shrem controls additional bitcoin addresses and holds additional bitcoin, but with the limited information we have, we are currently unable to identify these additional addresses. Shrem was an early adopter of bitcoin and has been a member of the community for years. As evidenced by our investigation, he utilizes multiple addresses, which suggests to us that other addresses belong to him which we have not been able to identify.

36. Based upon (a) the addresses we identified as being associated with Shrem, (b) our identification of addresses associated with bitcoin exchanges, and (c) our clustering techniques, we believe that Shrem has sent bitcoin to or received bitcoin from the following exchanges: Bitfinex, Bitstamp, BITTREX, BTC-e, Changelly, Coinbase, Cryptsy, Kraken, LiveCoin, Local Bitcoins, MtGox, Orderbook, Poloniex, and Xapo.

37. These exchanges should be able to confirm that Shrem holds accounts there, and likely can provide additional details concerning Shrem's deposits and withdrawals. This information would identify further addresses associated with Shrem.

Suspicious December 2012 Transaction

38. One string of transactions warrants particular note.

39. We were informed by WCF that they believed Shrem could not account for approximately 5,000 bitcoin that was owed to WCF between approximately September and October 2012.

40. A transaction with an address publicly acknowledged by Shrem received and sent 5,000 bitcoin in December 2012 — close proximity to the time WCF says that it failed to receive 5,000 bitcoin from Shrem.

41. Specifically, at 17:07 on December 31, 2012, Shrem's vanity address identified above — 1Shremdh9tVop1g xMzJ7baHxp6XX2WWRW ("1Shrem") — received 5,000 bitcoin. The identity of the owner of the sending address — 15kN4RRGAQapscJjSg1VEKbrWtNf192pwk — cannot be determined with presently available information, but the address has sent 6313.3 bitcoin to and received 50 bitcoin from addresses believed to belong to online exchange Coinbase, which could verify the owner of the sending/receiving account of those bitcoin. A true and correct copy of the transaction, downloaded from the blockchain, is attached hereto as Exhibit G.

42. The 5,000 bitcoin in 1Shrem subsequently moved approximately one hour later to another address — 1MQ3K9aPcEDCekpFBGyDAgtD1uPss8E7rY, the owner of which cannot be identified with presently available information. A true and correct copy of the transaction, downloaded from the blockchain, is attached hereto as Exhibit H.

43. The 5,000 bitcoin then sat in that address for approximately 11 months, when at 18:37 on November 3, 2013 it was sent to 1JMPofaycssfjTNUYXNzBFLHdNjJhwb9qn. Two minutes later, 2500 of these bitcoin were sent to an address believed to be associated with Coinbase. True and correct copy of these transactions, downloaded from the blockchain, are attached hereto as Exhibits I and J.

44. Nearly six months later, on April 20, 2014, 1499 of the remaining bitcoin were sent to an address believed to be associated with the online exchange Xapo. (The remaining 1001 bitcoin were distributed elsewhere). A true and correct copy of the transaction, downloaded from the blockchain, is attached hereto as Exhibit K.

45. We do not know if Shrem sent the bitcoin to Coinbase and Xapo, as there are two unidentified address between the transfer of the 5,000 bitcoin to Shrem and to the exchanges. Both exchanges would be able to identify the owner of the accounts that received the bitcoin on the exchanges.

46. We do suspect, however, that Shrem could control the unidentified addresses that sent the 5,000 bitcoin to the 1Shrem address, as well as the two subsequent addresses that received those funds and transferred the funds to addresses believed to belong to Coinbase and Xapo.

47. Both the address that initially sent the 5,000 bitcoin (15kN4RRGAQapscJjSg1VEKbrWtNf192pwk) as well as the address that sent 2500 bitcoin to an address believed to belong to Coinbase (1JMPofaycssfjTNUYXNzBFLHdNjJhwb9qn) sent money to the same address believed to belong to Coinbase. The pattern of these transfers could indicate that all of the addresses, as well as the Coinbase account, are owned and/or controlled by the same individual.

48. We have indicated to WCF that we could expand our investigation into Shrem's holdings if we were provided with additional information from the bitcoin exchanges, which would enable us to identify transactions into or out of any accounts held by Shrem on those exchanges, thereby enabling us to identify further addresses associated with Shrem.

I declare under penalty of perjury under the laws of the United States and the State of New York that the foregoing is true and correct to the best of my knowledge.

Executed on 8 September 2018 in Philadelphia, PA

Tom Robinson